REMARKS

The Office Action dated September 12, 2005 and the Advisory Action dated November 1, 2005 have been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 5, 15, 17, and 25 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 16 has been cancelled without prejudice or disclaimer. Support for the amendments may be found at least in the originally filed claims and in the specification on page 25, line 3 – page 26, line 21. Accordingly, no new matter has been added and no new issues are raised which require further consideration or search. Therefore, claims 1-3, 5-15, 17-19, 21-27, and 29-33 are currently pending in the application and are respectfully submitted for consideration.

In the Office Action, claims 1-4, 6-16, and 18-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Angelo (U.S. Patent No. 6,370,649). The Office Action took the position that Tello discloses all of the elements of the claims, with the exception of a host configured to receive a guess passcode from a manufacturer. The Office Action then relies upon Angelo as allegedly curing this deficiency in Tello. The rejection is respectfully traversed for the reasons which follow.

Claim 1, upon which claims 2-3 and 5-14 are dependent, recites an apparatus for enabling the functionality of a component. The apparatus includes a random number generating module for generating a random number, and a hash function module in communication with the random number generating module. The random number generating module includes a linear feedback shift register and a ring oscillator in communication with the hash function module, the linear feedback shift register being configured to output a random number. The apparatus further includes a host in communication with the random number generating module, at least one memory in communication with the host, an encryption module in communication with the memory, and a comparing device in communication with the encryption module and the hash function module. The comparing device compares a first bit string to a second bit string in order to generate a function enable output for the component. The at least one memory further comprises a guess register in communication with the host and the encryption module, the guess register being configured to receive a guess passcode from the host, and a public key module in communication with the encryption module, the public key module being configured to store a public key therein. The host is configured to receive a guess passcode from the manufacturer of the component.

Claim 15, upon which claims 17-19 and 21-24 are dependent, recites a component for selectively enabling a functionality of an electronic device. The component includes a means for generating a random bit string, a hash function module in communication with the means for generating, a means for acquiring a guess passcode in communication

with the means for generating, an encryption module in communication with the means for acquiring, and a comparing device in communication with the encryption module and the hash function module. The means for generating includes a random number generating module configured to receive an initiate signal and output a random number, and a linear feedback shift register, having an input and an output, and a ring oscillator. The comparing device has an output for transmitting a functionality enable signal therefrom. The encryption module further comprises a public key encryption module, and a public key module in communication with the public key encryption module. The public key encryption module is configured to receive a public key from the public key module and a guess passcode from the means for acquiring, and generate a ciphertext bit string therefrom. The means for acquiring the guess passcode is configured to acquire the guess passcode from the manufacturer of the electronic device.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on

electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, Tello and Angelo, whether viewed singly or combined, fail to disclose or suggest the elements of the claims, and therefore fails to provide the advantages discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who

lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that Tello and Angelo, whether viewed individually or combined, fail to disclose or suggest all of the elements of the presently pending claims. For example, neither Tello nor Angelo disclose or suggest a random number generating module comprising a linear feedback shift register and a ring oscillator in communication with a hash function module, the linear feedback shift register being configured to output a random number, as recited in claim 1. Similarly, both Tello and Angelo fail to disclose or suggest means for generating a random bit string comprising a random number generating module configured to receive an initiate signal and output a random number, where the means for generating further comprises a linear feedback shift register, having an input and an output, and a ring oscillator, as recited in claim 15.

As recited in claims 1 and 15, as discussed above, and supported by the specification, certain embodiments of the present invention provide a random sequence generator 36, which is configured to generate a random sequence of bits of a predetermined length (specification, page 25, lines 7-8 and Fig. 4). According to this

embodiment of the invention, a linear feedback shift register (LFSR) 37 is utilized in conjunction with a ring oscillator configuration 40 in order to generate the desired random number. The random sequence generator 36 is configured to receive a run signal at an input to the generator. This input indicates that the generator is to output a random number for use by the random id based enabler 41. After receiving a run signal and generating the desired random number, the random number is transmitted to the input of hash function module 29 as pre-image information. Additionally, the random number is communicated to host 18. More particularly, the run signal received by random sequence generator 36 is received at a first input of NAND gate 38. The output of NAND gate 38 is transmitted to an input of linear feedback shift register (LFSR) 37, as well as to the input of a series bank of inverters 39. The output of the series bank of inverters 39 is in communication with a second input of NAND gate 38. As a result of this configuration, as illustrated in Figure 4, upon receiving a run signal at the input to random sequence generator 36, the cooperative operation of ring oscillator 40 and LFSR 37 generate a random number at the output of random sequence generator 36 (specification, page 26, lines 1-21 and Fig. 4).

As mentioned above, according to an embodiment of the present invention, the random id based enabler 41 first receives a run signal at the input to the random sequence generator 36, which operates to initiate the generation of the desired random identification number. Once this random number is generated, it is transmitted to both hash function module 29 and host 18. Hash function module 29 receives the random

number as pre-image input and generates a hash value at the output of hash function module 29. This hash value is communicated to a second input 20b of comparator 20. Additionally, host 18, upon receiving the random number from to random sequence generator 36, contacts the manufacturer to obtain a guess passcode corresponding to the random number generated by random sequence generator 36. The manufacturer, having the private key corresponding to the public key of random id based enabler 41, generates a guess passcode corresponding to the public key of random id based enabler 41 from the private key and an encryption/decryption algorithm. The guess passcode generated by the manufacturer is then transmitted to host 18 (specification, page 27, lines 1-14).

Upon receiving the guess passcode from the manufacturer corresponding to the random number generated by the random sequence generator 36, host 18 transmits the guess passcode to guess register 19. Guess register 19 transmits the guess passcode to public key encryption module 35 as clear text, where the guess passcode is then encrypted with the public key stored in public key module 34 to generate cipher text at the output of public key encryption module 35. This cipher text, which, if the key obtained from host 18 is authentic, is calculated to match the hash value output from hash function module 29, is then transmitted to the first input 20a of comparator 20. Comparator 20 compares the calculated cipher text to the hash value generated by hash function module 29. If the cipher text matches the hash value, an enable signal is transmitted from the output of comparator 20 to an input of OR gate 23. Another input of OR gate 23 is again connected to a bonding option circuit 25 to generate a manual

override of random id based enabler 41 if required. Upon processing the inputs from comparator 20 and bonding option circuit 25, assuming that at least one of these inputs is a logical high signal, OR gate 23 outputs an enable functionality signal that is used to initialize enablement of the corresponding functionality (specification, page 27, line 14 – page 28, line 8). Therefore, according to the embodiment of the invention as discussed above and illustrated in Fig. 4, it is apparent that the need for programming or designing a unique component identification number into every component is removed.

Applicants respectfully submit that the cited prior art references of Tello and Angelo fail to disclose or suggest the configuration of the present invention, as discussed above. Specifically, Tello and Angelo fail to disclose or suggest the random number generating module of the present claims. The Office Action takes the position that Tello discloses a random number generating module because it discloses the use of an RSA algorithm (Office Action, page 5, lines 17-19). In addition, the Office Action asserts that Crouch, as will be discussed below, discloses the use of a linear feedback shift register to generate random numbers (Office Action, page 14, lines 11-14). Applicants respectfully disagree. Applicants respectfully submit that Tello and Angelo, even when combined with Crouch, fail to disclose or suggest a random number generating module which includes a linear feedback register and a ring oscillator in communication with the hash function module, as recited in claim 1 and similarly recited in claim 15.

Tello merely discloses, as discussed above, the use of an RSA algorithm. Tello fails to disclose or suggest that the RSA algorithm utilizes a random number generating

module, contrary to what is asserted in the Office Action. Davis only discloses that linear feedback shift registers may be implemented to provide pseudo-random patterns to sections of integrated circuit logic wherein "pseudo-random" means that the patterns created by an LFSR are repeatable for a given starting point. However, Tello, Crouch, and Angelo fail to disclose or suggest a random number generating module, which includes a linear feedback register **and a ring oscillator,** and is in communication with the hash function module. As discussed above, according to certain embodiments of the present invention, upon receiving a run signal at the input to random sequence generator 36, the cooperative operation of ring oscillator 40 and LFSR 37 generate a random number at the output of random sequence generator 36. Once this random number is generated, it is transmitted to both hash function module 29 and host 18. Hash function module 29 receives the random number as pre-image input and generates a hash value at the output of hash function module 29. As such, Applicants respectfully submit that Tello, Angelo and Crouch, whether considered individually or combined, fail to disclose or suggest the configuration of the present invention as recited in claims 1 and 15.

Similarly, Applicants respectfully submit that Tello and Angelo do not disclose or suggest a hash function module in communication with a random number generating module, as recited in present claims 1 and 15. The Office Action cites Tello as allegedly disclosing this limitation of the claims. However, Tello only discloses that an algorithm generates hash numbers H1, H2, H3 which are then encrypted to generate H1', H2', H3' (Tello, Column 8, lines 10-16). Tello does not disclose or suggest that the algorithm for

generating the hash numbers is in communication with a random number generating module. In the response to arguments section of the Office Action, it is alleged that the encrypted hash numbers constitute a random generating module in communication with the hash function module. Applicants respectfully disagree. According to the present invention, the generated random number is transmitted to the input of hash function module 29 as pre-image information (Specification, page 26, lines 10-13). Consequently, the hash function module receives a random number as an input and generates a hash value at the output of the hash function module 29 (Specification, page 27, lines 1-5). As such, the encrypted hash numbers of Tello cannot be considered to correspond to the random number generated in the present invention which is utilized to produce a hash value. In addition, Angelo also does not disclose or suggest that a hash function module is in communication with a random number generating module. Therefore, Tello and Angelo, whether viewed individually or combined, fail to disclose or suggest at least this element of claims 1 and 15.

For at least the reasons discussed above, Applicants respectfully assert that claims 1 and 15 recite limitations that are neither disclosed nor suggested by the cited prior art. Thus, Applicants respectfully request that the rejection of claims 1 and 15 be withdrawn.

Applicants note that claims 2-3, 5-14, 16-19, and 21-24 are dependent upon claims 1 and 15, respectively. Consequently, claims 2-3, 5-14, 16-19, and 21-24 should be allowed for at least their dependence upon claims 1 and 15, and for the specific limitations recited therein.

Claims 5 and 17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello in view of Angelo and further in view of Crouch (U.S. Patent No. 5,383,143). The Office Action took the position that Tello and Angelo disclose all of the elements of claims 5 and 17, with the exception of a linear feedback shift register, a NAND gate, and at least one inverter in communication with the linear feedback shift register and NAND gate. The Office Action then relies upon Crouch as allegedly curing these deficiencies in Tello and Angelo. The above rejection is respectfully traversed for the reasons which follow.

Tello and Angelo are discussed above. Crouch discloses a self re-seeding linear feedback shift register data processing system for generating a pseudo-random test bit stream. The data processing system 10 has a test controller 12 with a pattern generator 18 for receiving a seed value and generating many pseudo-random values from the seed value. A re-seed and compare circuit 22 monitors the pattern generator 12 and determines when the seed value repeats in the pseudo-random number sequence generated by the generator 18. Once the compare circuit 22 determines that the seed value has repeated, the control circuit 20 allows the generator 18 to clock once more and latches a new seed value into the circuit 22.

Applicants note that claims 5 and 17 are dependent upon claims 1 and 15, respectively. Further, as discussed above, the combination of Tello and Angelo fails to disclose or suggest all of the elements of claims 1 and 15. Additionally, Crouch fails to cure those deficiencies in Tello and Angelo. As such, claims 5 and 17 should be allowed

for at least their dependence upon claims 1 and 15, and for the specific limitations recited therein.

Claims 25-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis (U.S. Patent No. 5,577,121) in view of Tello and further in view of Angelo. The Office Action took the position that Davis discloses all of the elements of the claims, with the exception of the second bit string being encrypted using a public key and receiving the second bit string from a manufacturer of the electronic component. The Office Action then relies upon Tello and Angelo as allegedly curing this deficiency in Davis. The rejection is respectfully traversed for the reasons which follow.

Claim 25, upon which claims 26-27 and 29-33 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of generating a random number, calculating a first bit string from the random number, determining a second bit string corresponding to the random number, encrypting the second bit string with a public key to generate a third bit string, comparing the third bit string to the first bit string to determine a match, and outputting a function enable signal in accordance with the comparison. The step of generating a random number includes receiving an initiate signal at a random number generating module and outputting a random number, wherein the random number generating module includes a linear feedback shift register and a ring oscillator. The encrypting step further comprises the steps of receiving a guess passcode from a host, receiving a public key, and encrypting the guess passcode and the public key to generate a ciphertext bit string. The step of

determining the second bit string comprises receiving the second bit string from the manufacturer of the electronic component.

Tello and Angelo are discussed above. Davis discloses a transaction system for integrated circuit cards, and more specifically it discloses a method of conducting a transaction between an integrated circuit (IC) card and a transaction terminal which includes a security module. The method includes establishing communication between the terminal and the IC card and separately generating a session key in the IC card using data stored in the IC card and a code associated with the particular IC card and in the security module using data stored in the security module and the code associated with the particular IC card. The session key generated by the IC card is used to encrypt data using an encryption algorithm to obtain a first result and the session key generated by the security module is used to encrypt the same data using the same encryption algorithm to obtain a second result. The first and second results are compared and the terminal will conduct the transaction only if the comparison establishes that the first result and the second result are identical.

Applicants respectfully submit that the combination of Davis, Tello and Angelo fails to disclose or suggest all of the elements of claim 25. More specifically, Applicants respectfully submit that the cited references fail to disclose or suggest "generating a random number, wherein said step of generating a random number further comprises the steps of receiving an initiate signal at a random number generating module and outputting a random number, wherein the random number generating module comprises a linear

feedback shift register and a ring oscillator," as recited in claim 25. As discussed above with respect to claims 1 and 15, both Tello and Angelo fail to disclose or suggest a random number generating module which includes a linear feedback register and a ring oscillator. In addition, Davis also fails to cure these deficiencies in Tello and Angelo since Davis also fails to disclose or suggest such a random number generating module. Davis, like Tello and Angelo does not disclose or suggest that the random number generating module includes a linear feedback register and a ring oscillator.

Furthermore, Applicants respectfully submit that Davis, Tello, and Angelo all fail to disclose or suggest determining a second bit string corresponding to the random number, as recited in claim 25. The Office Action cites Davis as allegedly disclosing this element of the claim. Applicants submit that Davis does not determine a second bit string which corresponds to the random number. Rather, according to Davis, the security module generates a random number and sends it to the SVC. The SVC encrypts the random number with the SVC session key. The security module encrypts the random number with the security module session key (Davis, Column 13, lines 6-52). Therefore, Davis only discloses generating a random number which is then encrypted by the SVC and security module. Davis does not disclose that a second bit string corresponding to the random number is determined.

Therefore, Davis, Tello and Angelo, whether considered singly or combined, fail to disclose or suggest all of the elements of claim 25. As such, Applicants respectfully request that the rejection of claim 25 be withdrawn.

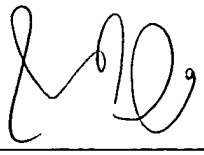
It is also respectfully submitted that claims 26-27 and 29-33 are dependent upon claim 25 and therefore should be allowed for at least their dependence on claim 25, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unobvious. It is therefore requested that all of claims 1-3, 5-15, 17-19, 21-27, and 29-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf

Enclosures: Request for Continued Examination